United States District Court

for the
Western District of New York

United States of America

v.

NIKITA ANDREEVICH SKLYUEV

Defendant

Case No. 21-mj-1102

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Between on or about September 25, 2018 and on or about February 22, 2019, in the County of Erie, in the Western District of New York, the defendant devised and intended to devise a scheme and artifice to defraud Victim 1, a person known to the government, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, in violation of Title 18, United States Code, Section 1343. It was part of the scheme that the defendant stole the private key to the EOSIO Wallet Explorer of Victim 1, making Victim 1's cryptocurrency valued at more than $11 million inaccessible to Victim 1. The defendant then stole the cryptocurrency by transferring it to other wallets controlled by the defendant. For the purpose of executing the scheme and artifice described above, and attempting to do so, the defendant caused to be transmitted by means of wire communication in interstate commerce signals and sounds, to wit: on or about February 22, 2019, the defendant transferred cryptocurrency from the EOSIO Wallet Explorer of Victim 1 in three separate electronic transfers.

All in violation of Title 18, United States Code, Section 1343.

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

Complainant's signature
ADAM HAMILTON
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Sworn to before me and signed in my presence.

Date: April 28, 2021

Judge's signature
HON. JEREMIAH J. McCARTHY
UNITED STATES MAGISTRATE JUDGE
Printed name and title

City and State: Buffalo, New York

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, ADAM HAMILTON, being duly sworn, depose and state the following:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have served in this capacity since September 2017. I am currently assigned to the Cyber Squad, Buffalo Division, in Buffalo, New York and I have worked cyber matters, that is, matters focused on computer intrusions. I have also received extensive training on cyber matters during my time in the Bureau. I have worked and assisted with matters involving unauthorized access to computer systems, internet fraud, business email compromises, ransomware intrusions, and darknet vendors. Prior to my employment in the FBI, I received a Bachelor's of Science in Computer Science and Engineering.

2. I make this affidavit in support of an application for a criminal complaint and arrest warrant charging, NIKITA SKLYUEV, with a violation of Title 18, United States Code, Section 1343 (Wire Fraud), three counts.

3. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the purpose of establishing probable

cause to believe an offense has been committed, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause.

II. RELEVANT STATUTES

4. Wire Fraud: Title 18, United States Code, Section 1343 makes it a federal crime to devise or intend to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

III. PROBABLE CAUSE

5. In June 2019, an individual investor identified throughout as Victim 1 contacted the FBI to report that between on or about September 25, 2018 and on or about February 22, 2019, the exact date being unknown, the theft of 11.8 million USD in EOS[1] cryptocurrency occurred from his EOS Account known throughout as "gm3dcnqgenes". Victim 1 attributed the theft to the installation of the mobile application EOSIO Wallet Explorer on his personal iPhone.

[1] EOS is a cryptocurrency similar in nature to Bitcoin in that it is a decentralized form of virtual money into which any individual can invest fiat currency.

6. After installation of the EOSIO Wallet Explorer, Victim 1 lost control of his private key which was used to control access to the cryptocurrency. A private key is a form of verification, similar to a password, allowing only the holder access to the funds. Once Victim 1 lost control of his private key, the defendant later was able to initiate three transfers of the EOS cryptocurrency into accounts inaccessible to Victim 1.

7. Additional online searches of the application EOSIO Wallet Explorer identified more open source complaints from victims, indicating that upon installation and creation of their accounts, they also lost control of their private keys followed by unauthorized transfers of their EOS cryptocurrency.

8. Victim 1 reported his inability to access his cryptocurrency to the EOSIO Core Arbitration Forum ("ECAF"). ECAF was the governing body that arbitrated over the EOS Core and Community. ECAF accepted and ruled upon disputes, interventions, and assertions related to the exchange of EOS cryptocurrency and their respective owners.

9. In October 2018, Victim 1 initiated a claim with ECAF indicating the theft of his EOS cryptocurrency. After providing appropriate identifying documentation, proof of ownership of the initial account "**gm3dcnqgenes**" and initial investment into the EOS, ECAF arbitrators determined that Victim 1 was indeed the rightful owner. The ECAF ruling held that Victim 1 was the rightful owner of the transferred EOS and required cryptocurrency exchanges currently holding the EOS in question to reinstate control back to an account controlled by Victim 1.

10. Victim 1 also hired a forensic analysis team to track the final destination of his EOS cryptocurrency by following the transfers of EOS on the EOS Blockchain[2]. The team identified multiple wallets that assumed control of Victim 1's EOS. One wallet, "**Binancecleos**", was identified on the Binance exchange. Another wallet, "**Bitfinexdep1**", was identified on the Bitfinex exchange.

11. It was determined that on or about February 22, 2019, 2,092,395.5356 EOS, valued at approximately $11.8 million fraudulently was transferred from Victim 1's account "**gm3dcnqgenes**" in three separate transfers to another account known as "**newdexmobapp**". These three fraudulent transfers each constituted a violation of Title 18, United States Code, Section 1343 [Wire Fraud].

12. The 2,092,395.5356 EOS was then dispersed among multiple accounts until a portion totaling 966,124.7828 EOS was cashed out using multiple virtual currency exchanges at the time. Of the 966,124.7828 EOS, 711,124.7828 EOS had been transferred to the account "**Binancecleos**" on the Binance exchange. 100,000 of the original 2,092,395.5356 EOS was transferred to the account "**pnsdiia1pcuy**" and 155,000 of the original 2,092,395.5356 EOS was transferred to the account "**geydddsfkk5e"**. Of this 255,000 EOS, 158,000 was finally transferred to the account "**Bitfinexdep1**" on the Bitfinex exchange. The remaining 1,126,270.7528 EOS is still located in wallets controlled by the subject waiting to be cashed out through either a virtual currency exchange or exchange service.

[2] The blockchain is a virtual ledger tracking all transactional information using multiple verifications to assure the transfers have occurred between corresponding virtual addresses.

13. On the Binance exchange, the following accounts were identified as receiving stolen EOS:

Memo:	103528664	Email:	5320xmb@gmail.com	Name:	Ihor	Morozov
Memo:	108930609	Email:	se@ychanger.net	Name:	Anastasiya	Yunusova
Memo:	108957575	Email:	info@ychanger.net	Name:	Sergei	Nikolaevich
Memo:	107177674	Email:	petroffsyn@gmail.com	Name:	Nikolai	Nikitin
Memo:	103358974	Email:	stkhir@gmail.com	Name:	Stepan	Tkhir
Memo:	104844035	Email:	zoranamartovic@gmail.com	Name:	Zoriana	Martovych

14. I spoke with the owners of the ychanger.net accounts, Anastasiya Yunusova and Sergei Nikolaevich; as well as Stepan Tkhir, owner of the stkhir@gmail.com account; and Nikolai Nikitin, owner of the petroffsyn@gmail.com account. The owners of all four accounts responded that they worked for various virtual currency exchange services. Anastasiya Yunusova and Sergei Nikolaevich worked for ychanger.net, Stepan Tkhir worked for 24bestex.com, and Nikolai Nikitin worked for cointocard.org. All exchanged the received EOS into Ethereum, another cryptocurrency. All four also stated they received the requests from the email account **gleb001501@gmail.com**.

15. The **gleb001501@gmail.com** email was examined via a search warrant (Case No: 19-MJ-175) issued by the United States District Court for the Western District of New York. Contents of the email revealed it was utilized by NIKITA SKLYUEV, a citizen of Uzbekistan, as his personal email account.

16. Contents of the email identified messages confirming transactions of EOS into Ethereum from cointocard.org and ychanger.net. This information matched information provided by those organizations.

17. Also found within the Google Drive for the gleb001501@gmail.com account was a Microsoft Word document written in Uzbek. Upon translation of the document by the Federal Bureau of Investigation (FBI), the document outlined details of how SKLYUEV acquired control of Victim 1's wallet **gm3dcnqgenes**, and how he traveled to Ukraine to meet with another individual to discuss the matter.

18. A request for information was sent to the Ukraine's Security Service (SBU) in regard to this information. In a response received via the FBI Legal Attaché located in Kiev, the SBU confirmed that SKLYUEV recently traveled to, and is currently staying in, Odessa, Ukraine.

19. A subpoena return from Apple for the application EOSIO Wallet Explorer and SKLYUEV's iCloud account indicated that they shared identical IP address logins with the email account **gleb001501@gmail.com**. Subscriber information on the EOSIO Wallet Explorer application listed the owner as a Valeriy Dorojkin with email **myvito20154@yandex.ru**. However, the subscriber for the telephone number associated with the **myvito20154@yandex.ru** account was SKLYUEV.

20. As a part of the Google search warrant return, Google identified additional accounts that were linked to **gleb001501@gmail.com** through SMS registration. SMS registration is used to identify accounts that are tied to the same phone number, linking them to the same owner. The Mobile telephone number +998 915515522 was the mobile number registered by **gleb001501@gmail.com**.

21. Open source research on this number identified accounts tied to SKLYUEV, including a Skype account with display name NIKITA SKLYUEV. In addition, telephone number +998 915515522 was also identified by Google as being used to register the email **myvito20154@yandex.ru** account, the same email associated with the creation of the EOSIO Wallet Explorer software.

IV. CONCLUSION

22. In summary, given the aforementioned facts, there is probable cause that NIKITA SKLYUEV participated in a scheme to fraudulently obtain EOS cryptocurrency using a malicious mobile application and exchanging that cryptocurrency into Ethereum to hide its point of origin.

23. Based on the foregoing, I believe there is probable cause to believe NIKITA SKLYUEV engaged in a violation of Title 18, United States Code, Section 1343, wire fraud, as he participated in a scheme and artifice to defraud Victim 1 of millions of dollars of EOS cryptocurrency.

ADAM HAMILTON
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before

me this 28th day of April, 2021.

HON. JEREMIAH J. MCCARTHY
United States Magistrate Judge